Office of Federal Student Aid
Department of Education

Security Risk Assessment For Conditional Disability Discharge Tracking System (CDDTS)

DRAFT

August 15, 2003

Prepared by:
Accenture

TABLE OF CONTENTS

1.0 INTRODUCTION **3**

1.1 Background 3
1.2 Purpose of this report 3
1.3 Scope 4
1.4 Report Organization 4

2.0 RISK ASSESSMENT APPROACH **5**

2.1 Step 1 – Define System Boundary 5
2.2 Step 2 – Gather Information 6
2.2.1 Interviews *6*
2.2.2 Site Visit *7*
2.2.3 Documentation *7*
2.2.4 Network Scanning *7*
2.3 Step 3 – Conduct Risk Assessment 7
2.3.1 Documenting Vulnerabilities *8*
2.3.2 Impact *9*
2.3.3 Likelihood *10*
2.3.4 Risk *12*

3.0 SYSTEM CHARACTERIZATION **13**

3.1 System Overview 13
3.2 System Interfaces 15
3.3 Data 17
3.4 System and Data Criticality and Sensitivity 17
3.4.1 Criticality *17*
3.4.2 Sensitivity *17*
3.4.2.1 Confidentiality: **High** 17
3.4.2.2 Integrity: **Medium** 17
3.4.2.3 Availability: **Medium** 17
3.5 Users 18

4.0 THREAT STATEMENT **19**

4.1 Threat Sources 19
4.2 Threat Actions 20

5.0 FINDINGS **21**

EXECUTIVE SUMMARY

The mission of the Department of Education's Conditional Disability Discharge Tracking System (CDDTS) is to record and track borrowers who have requested that their loans be discharged due to total and permanent disabilities.

The risk assessment described in this report was performed by Accenture under Task Order 120 – Security and Privacy Support (period of performance January 1, 2003 to December 31, 2003).

To identify the potential threats and vulnerabilities associated with the CDDTS, Accenture gathered information through the following techniques:

- Document review,
- Site visits to the CDDTS data center,
- Interviews with designated FSA management and technical personnel, and
- Interviews with ACS contractors.

This report documents risk assessment activities in the following security domain areas:

- Management Security,
- Operational Security,
- Technical Security, and
- Administrative Security.

A total of 21 observations were made in the areas of management, operational, technical, and administrative security. Table ES-1 presents these observations, providing observation numbers and descriptions, as well as associated risk levels. The risk associated with each observation is described as high, medium, or low, as defined below. The risk level represents the degree or level of risk to which FSA assets and resources may be exposed.

High Risk Findings: 4. High risk indicates that a threat is at least moderately likely to exploit the identified vulnerability, and such exploitation is likely to severely and adversely affect CDDTS tangible and intangible resources. This level of risk indicates a strong need for corrective measures and actions, and a plan must be developed to incorporate these actions within a reasonable period of time.

Medium Risk Findings: 15. Medium risk indicates that exploitation of the identified vulnerability by a threat is possible, and such exploitation is likely to affect CDDTS significantly, indicating the loss of some tangible assets or resources, which could impede the CDDTS's mission, reputation, or interest. This level of risk indicates corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

Low Risk: 2. Low risk indicates that the identified weaknesses may be subject to exploitation by a threat, but the probability of exploitation is low, and the impact on FSA would be minor. This level of risk indicates that FSA management should be cautioned and corrective measures applied where required.

Appendix A details the observations, presenting the observation number and description, vulnerabilities and threats, potential impacts, likelihood, priority, and recommendations for each observation.

OBSERVATION NUMBER	VULNERABILITY DESCRIPTION	RISK LEVEL
Management Security		
M1	Security testing of changes is not part of the CDDTS configuration management plan.	Medium
M2	Anti-virus tools are not run on the CDDTS server.	Medium
M3	Security training during employee orientation is brief and not documented.	Medium
M4	Disaster recovery plans have not been tested.	Medium
M5	Business continuity plans have not been tested.	Medium
M6	A security training and awareness program has not been fully implemented.	Medium
M7	Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a third party.	Medium
M8	Security risk analysis and testing is not included in the configuration management plan.	Low
M9	Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.	Low
Operational Security		
O1	Authorized access is not reviewed annually.	Medium
Technical Security		
T1	Audit trail logging and review are not routinely performed.	High
T2	User passwords for the CDDTS application are stored in clear text.	High
T3	There are no functions to detect and lock accounts after repeated login failure.	High
T4	The System Security Plan does not specify periodic scanning for unauthorized modems.	High
T5	An Intrusion Detection System is not yet fully implemented.	Medium
T6	Firewall policies and filtering rules should be audited.	Medium
T7	CDDTS accounts are not configured for automatic logout after periods of inactivity.	Medium
T8	Some file transfers to CDDTS are made through standard FTP.	Medium
Administrative Security		
A1	No CDDTS asset inventory.	Medium
A2	A FISMA Privacy Impact Assessment not performed.	Medium
A3	The System Security Plan is missing required content.	Medium

Table ES-1

1.0 INTRODUCTION

1.1 BACKGROUND

The Conditional Disability Discharge Tracking System (CDDTS) allows the U.S. Department of Education – Office of Federal Student Aid (FSA) to record and track borrowers who have requested that their loans be discharged due to total and permanent disabilities. Regulations require that all such loans be recorded and tracked for a period of three years from the date of disability, as certified by a physician, before being discharged.

Student loan borrowers who are unable to work because of injury or illness that permanently affects their ability to repay student loans may submit a disability discharge application. Required supporting documentation includes a physician certification of the indefinite nature of the disability, loan promissory notes, an assignment form, the discharge application, payment history, as well as other supportive documents. The borrower's application for disability discharge is entered into CDDTS, and the information is tracked for three years to satisfy regulatory requirements. During this time, the borrower's eligibility for disability discharge is followed before final discharge is granted. Eligibility requirements include an income that does not exceed the poverty guidelines of the borrower's state, and that no new Title IV loans are received.

CDDTS was developed and is currently operated under contract by ACS. The CDDTS server components are housed in the ACS Data Center in Rockville, MD.

1.2 PURPOSE OF THIS REPORT

The purpose of this report is to provide the Department of Education and FSA management with an assessment of the adequacy of the management, technical, operational and administrative security controls used to protect the confidentiality, integrity, and availability of CDDTS. This risk assessment report identifies threats and vulnerabilities applicable to CDDTS; the impact associated with these threats and vulnerabilities; the likelihood that a vulnerability will be exploited; countermeasures in place to mitigate the risk; and the existence of any residual risk.

This report documents the risk assessment activities that Accenture[1] performed from July 17, 2003 to August 15, 2003. Its goal is to help FSA management understand the security posture of CDDTS and its risk exposure. This risk assessment is part of FSA's continuing effort to ensure compliance with Federal policies, laws and guidance as well as the FSA IT Security and Privacy Policy.

[1] Accenture personnel have not been involved with the development or operation of CDDTS.

1.3 SCOPE

This risk assessment is limited to the Conditional Disability Discharge Tracking System, which consists of a single production server running the CDDTS application components and an Oracle database on the Windows 2000 Advanced Server operating system. The production server and associated development servers are housed in the ACS data center in Rockville, MD. The primary users of CDDTS are customer service representatives in the CDDTS Call Center in Utica, NY.

The risks were evaluated in the following security domains:

- Managerial,
- Technical,
- Operational, and
- Administrative

Site visits were conducted to the ACS office facility at 4 Choke Cherry Rd, Rockville, MD, and the ACS Data Center building at 1 Curie Court, Rockville, MD.

1.4 REPORT ORGANIZATION

This document is divided into four sections and an Appendix. Section 1 is the introduction. The remainder of the document consists of the following sections:

- Section 2 provides a description of the risk assessment methodology used by Accenture;
- Section 3 describes the characteristics of CDDTS including the hardware, software, connectivity, data, and system users; and
- Section 4 provides an analysis of the findings in the management, technical, operation, and administrative security domains.

Additionally, the document contains an appendix that provides the details of the risk assessment.

2.0 RISK ASSESSMENT APPROACH

Risk was evaluated qualitatively, meaning that numerical values were not assigned. Instead a rating of high, medium, or low was provided. The Accenture risk assessment methodology involved three major steps that are described below.

- Step 1 – Determine System Boundary
- Step 2 – Gather Information
- Step 3 – Conduct Risk Assessment.

The methodology used by Accenture to perform the risk assessment for CDDTS to the guidelines developed by the Office of Federal Student Aid (FSA), which in turn is based on the following federal guidelines:

- National Institute of Standards and Technology (NIST) Special Publication 800-30, *Risk Management Guide for Information Technology Systems* (Draft).
- Office of Management and Budget (OMB) Circular A-130 "Security of Federal Automated Information Systems."

The level of risk was assessed by evaluating all collected risk-related attributes regarding threats, vulnerabilities, assets and resources, current controls, and the associated likelihood that a vulnerability could be exploited by a potential threat and the impact (e.g., magnitude of loss resulting from such exploitation).

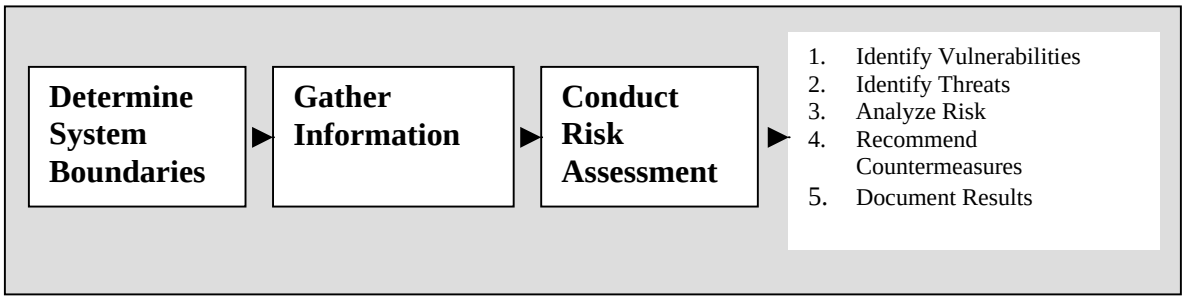

Figure 1: Risk Assessment Approach

2.1 STEP 1 – DEFINE SYSTEM BOUNDARY

The CDDTS system boundaries, which determine the risk assessment scope, were defined as the following components:

- CDDTS software: application code, Oracle 8i database system, Windows operating system
- Hardware: CDDTS production server, CDDTS development server, firewalls and other network components, Call Center workstations

- Physical facilities: ACS data center in Rockville, MD, ACS support offices in Rockville, MD, CDDTS Call Center in Utica, NY

The CDDTS system boundaries were established by reviewing the CDDTS design documentation and ACS network documentation, through discussions with the ACS project manager for CDDTS, and in consultation with the FSA system manager for CDDTS.

2.2 STEP 2 – GATHER INFORMATION

Accenture assessed CDDTS based on FSA security risk assessment guidelines, FSA support personnel understanding of the CDDTS operational environment, and FSA and Department-wide information technology (IT) policies and guidelines.

Information about CDDTS technical and procedural security controls was gathered through interviews with FSA system personnel, interviews with contractor personnel responsible for developing and operating CDDTS, site visits, and review of CDDTS technical and operational documentation.

2.2.1 Interviews

To collect information about CDDTS business functions, technical design, security controls, and operational procedures, interviews were conducted with several FSA and contractor support personnel. Interviews were based on the requirements and standards from the following sources:

- Sample Baseline Security Requirement, FSA Security Risk Assessment Guideline, Appendix F, February 2002
- Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26, November 2001
- FSA IT Security and Privacy Policy
- Accenture Security Risk Assessment Methodology

Interviews were conducted in person and by telephone, with follow-up questions submitted through email. Personnel who were interviewed or participated in site visits included the following:

- Denise Leifeste, CDDTS System Manager
- David Yang, CDDTS System Security Officer
- Raj Raghu, ACS Project Manager for CDDTS
- Maylon Hayes, ACS Production Environment Manager
- Brian Kissel, ACS Technical Support
- Michael Groover, ACS System Manager
- Abner Sangalan, ACS Data Center Operator
- Ray Baker, ACS Facilities Manager

2.2.2 Site Visit

The Accenture assessor made a site visit to the ACS support offices and data center in Rockville, MD on July 17, 2003. The facilities visited included the main ACS office support facility at 4 Choke Cherry Rd, Rockville, MD, and the ACS Data Center building at 1 Curie Court, Rockville, MD. The data center tour included observation of physical security controls, security procedures for visitors, surveillance measures, tape handling procedures, and system monitoring display consoles.

2.2.3 Documentation

The team reviewed all relevant information security (INFOSEC) documents in order to develop a better understanding of CDDTS. Listed below are all system and organizational documents reviewed in support of the assessment:

- CDDTS System Security Plan
- CDDTS Design Summary, June 15, 2002
- Department of Education GSS & MA Inventory Submission Formb
- CDDTS Configuration Management Document, August 2002
- CDDTS Business Continuity and Disaster Recovery Plan, August 2002
- Call Center Site Visitation, June 23, 2002
- CDDTS Tape Handling Policy and Procedure, July 2002
- CDDTS Production Network Diagram
- ACS Rockville Data Center Network Diagram
- FMS Application Setup for Conditional Disability Discharge Tracking System Processing

2.2.4 Network Scanning

Network scans were not conducted during the CDDTS risk assessment.

2.3 STEP 3 – CONDUCT RISK ASSESSMENT

The risk assessment encompassed the following subtasks:

- Compiling the Vulnerability List,
- Identifying and associating potential threats to vulnerabilities,
- Determining risks, and
- Developing countermeasure recommendations

The value of CDDTS is measured in terms of the criticality and sensitivity of the system and its data.

To assess risks to CDDTS, the Accenture risk assessment team identified a list of potential vulnerabilities that could be exploited by natural, environmental, human, or

administrative threats. Section 3 provides an analysis of the possible threats and threat agents that could exploit vulnerabilities in CDDTS.

Section 4 and Appendix A presents the findings and includes a discussion of the threat and vulnerability pair, impact and likelihood analysis, risk rating, and recommended countermeasures.

In order to determine risk the team identified the impact an exploited vulnerability would have on the system and the likelihood of the vulnerability being exploited. The following sections provide descriptions of vulnerabilities, impact, likelihood, and an overall risk matrix.

2.3.1 Documenting Vulnerabilities

Upon completion of the documentation reviews, testing, etc. we documented each identified vulnerability in Appendix A of the assessment. Once our list of vulnerabilities was complete, we categorized the identified vulnerabilities into the following four primary security areas

- Management Security,
- Operational Security,
- Technical Security, and
- Administrative Security

Based on NIST Special Publication 800-18, we determined to which category the vulnerability most appropriately belonged.

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. There was one finding in the area of management security.

The **operational** controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). Often, they require technical or specialized expertise and rely upon management activities as well as technical controls. There were a total of 3 findings in the area of operational security.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. There were a total of 4 findings in the area of technical security.

Administrative controls focus on regulatory and policy issues that do not fit easily into the other three categories. These controls reflect specifically mandated documentation, actions, or decisions a system owner must address to adequately implement security policy, both at the federal and department level.

2.3.2 Impact

Impact refers to the magnitude of potential harm that may be caused by threat exploitation. It is determined by the value of the resource at risk, both in terms of the information sensitivity and its importance to the Department's mission (i.e., criticality). The criticality and sensitivity of both the system and data are useful guides for assessing the potential impact of an exploited vulnerability. The table below provides a general description of impact.

Impact	Description
High	May result in the *loss* of significant information, or information resources. May significantly disrupt or impede FSA's mission or seriously harm its reputation or interest.
Medium	May result in the *loss of some* tangible assets, information, or information resources. May disrupt or harm the FSA mission or harm its reputation or interest.
Low	May result in the *loss of minimal* tangible assets, information, or information resources. May adversely affect the CDDTS mission, reputation, or interest.

Table 1: Impact Description

To determine impact, we compared the CDDTS sensitivity and criticality.

- Sensitivity takes into account the Confidentiality, Integrity and Availability.
- Criticality is the system's impact to the agency, and is rated at either Mission Critical, Important or Supportive

First we reviewed the sensitivity rating determined during the inventory review. For each identified vulnerability and associated threat, we determined which sensitivity category might have been impacted if the vulnerability was exploited. Certain threats did not impact every category; rather, only certain categories were impacted. For example, a denial of service attack may only impact availability, but confidentiality or integrity remained unaffected. In this case the sensitivity level was based solely upon your availability rating. Another example is the vulnerability of unencrypted data, where the threat may impact confidentiality and integrity, but not availability. In this case, we would choose the higher rating of confidentiality or integrity.

The criticality rating we used was extracted from the recent inventory review worksheet. After conducting a brief review of the rationale for our rating, we established the criticality rating of CDDTS to be Mission Important.

For each vulnerability/threat pair we took our sensitivity rating (High, Medium, Low) and our criticality rating (Critical, Important, Supportive) and input them into the matrix shown in Table 2 to determine the impact rating.

The impact for a threat/vulnerability combination was calculated as follows:

1) Sensitivity: Confidentiality (H/M/L), Availability (H/M/L) Integrity (H/M/L) = Overall Rating: H/M/L

2) Criticality: Mission Critical, Important, Supportive
3) Impact: High, Medium Low

Sensitivity X Criticality = Impact.

	System Criticality		
Information Sensitivity	*Mission Critical*	*Mission Important*	*Mission Supportive*
High	High	High	Medium
Medium	High	Medium	Medium
Low	Medium	Medium	Low

Table 2: Impact Description

The results of our impact analyses are documented as part of the Risk Assessment Matrix found in Appendix A of this document.

2.3.3 Likelihood

Likelihood is determined by considering threats and vulnerabilities. The likelihood that vulnerability will be exploited by a threat can be assessed and described as High, Medium, or Low. Factors that govern the likelihood of threat exploitation include threat capability, the frequency of threat occurrence, and effectiveness of current countermeasures. Generally, the likelihood of a threat exploiting vulnerability can be described as presented in the table below.

Likelihood	Description
High	The capability of the threat is significant, and/or countermeasures to reduce the probability of threat exploitation are insufficient.
Medium	The capability of the threat is moderate, and implemented countermeasures lessen the probability of threat exploitation.
Low	The capability of the threat is limited, and countermeasures are in place effectively reducing the probability of threat exploitation.

Table 3 – General likelihood description

To assess the likelihood of a threat exploiting a vulnerability, we divided likelihood into two components: Threat Capability and Countermeasure Effectiveness. The matrix below illustrates the relationship of a threat or threat agent to the capabilities of the threat or threat agent, and the existing countermeasures employed to guard against the threat. For the purposes of these analyses, capabilities are defined as the inherent difficulty in acting out the threat regardless of any existing countermeasures.

Threats	Capabilities	Countermeasures
Natural	**Location Based H/M/L**	**Building codes, cold sites**
Environmental	**History Based H/M/L**	**Back-ups, redundancies**
Human	**Access based H/M/L**	**Firewalls, guards, IDS, audit logs, RoB**
Administrative	**H**	**Documentation**

Table 4 – Likelihood matrix

If a threat was determined to be of natural origin (i.e. tornado, hurricane, flood, etc), the capabilities of the threat were based upon the geographic location of the system (and therefore the vulnerability in question). For example, the threat of hurricanes in Florida is much greater than the threat of a hurricane in Oklahoma. Therefore, a system located in Florida would have a high likelihood of a hurricane occurring as opposed to Oklahoma. However, the inverse can be said for tornados in Oklahoma.

For purposes of our analyses, environmental threats were constrained to an historical perspective. For example, the question was asked, "How many times has the heating and cooling system ever failed in the past year?" If the answer is 0, the rating was low; 1-2, the rating was medium; 3 or more, the rating was high.

Because of the wide variety of human threat agents, determining the threat capabilities of a human agent depended on the vector of the threat. Essentially, human threats could be broken down into numerous subcategories, the most important for this exercise being external vs. internal, and network vs. physical. If the threat was an external agent using network access, the capability was rated as high due to the sheer volume of attempted network attacks against all government systems. If no external access was available, the network threat capability was reduced to medium due to the potential existence of disgruntled employees, unintentional errors, etc. If the threat was of a more physical nature (theft, vandalism, sabotage, etc.), the capability was rated by the difficulty in carrying out the attack.

Administrative threats, due to the constant reviews and audits conducted by the IG, GAO, OMB, and Departmental teams, were given a high capability rating. We assumed that our system's administrative deficiencies would be discovered by at least one of these groups, requiring urgent compliance to the applicable standards or policies.

After determining the capability of the threat, we analyzed the existing countermeasures we employed to guard against the threat. For example, if our system was located in Florida, specific building codes would be established to protect against a hurricane. To

measure the effectiveness of the system's countermeasures, we used the following subjective scale.

- If our assessment indicated we employed numerous measures to combat the specific threat and were confident in the their effectiveness, we rated the countermeasures effectiveness as high.
- If our assessment indicated we did not do much to address this particular threat and found our countermeasures lacking or non-existent, we rated the countermeasures as low.
- If our assessment indicated a moderate level of controls, more than low and less than high, we rated the countermeasures as medium.

Once the threat capability and countermeasure effectiveness were assessed for each vulnerability/threat pair, we used the matrix below to determine the overall likelihood of the threat exploiting the vulnerability. The findings were documented in Appendix A of this risk assessment.

	Countermeasure Effectiveness		
Capability	*High*	*Medium*	*Low*
High	Medium	High	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Table 5: Likelihood Rating

2.3.4 Risk

After evaluating likelihood and impact, the risk assessment team employed a risk scale matrix with the ratings of high, medium, and low to determine the degree or level of risk to which a system, facility, or procedure might be exposed if a vulnerability were exploited by an associated threat. The level of risk equals the intersection of the likelihood and impact values. For example, suppose the likelihood level is High and the impact level is Low for the threat/vulnerability pair. Based on the risk matrix found below, there would be a Medium risk level.

Risk = Impact X Likelihood

	Likelihood		
Impact	***High***	***Medium***	***Low***
High	High	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Table 6: Risk Rating

3.0 SYSTEM CHARACTERIZATION

3.1 SYSTEM OVERVIEW

The Conditional Disability Discharge Tracking System (CDDTS) was created to provide information services to the Conditional Disability Discharge (CDD) Program. CDD was created to support the regulatory requirement to track borrower claims for total and permanent disability discharge for three years.

The business processing requirements for CDDTS are based on the following financial assumptions:

- No receivables will be established for loans received by CDD.
- Borrowers determined to be ineligible will be returned to active servicing status.
- When it becomes necessary to resume servicing on a conditionally discharged loan, CDD will transfer the loan to AFSA's proprietary FFEL or Perkins servicing system; to the Direct Loan servicing system; or to FSA's Debt Collection System (DCS), as appropriate.

CDD must maintain copies of Deposit Tickets (SF215), Debit Memos (SF5515) for Insufficient Funds (NSF) or other deposit adjustments on a daily basis. FSA Accounting will be sent a copy of the daily log when a collection is received. The CDD system must maintain detailed records of all transactions, including cash receipts, disbursements, and adjustments by borrower name, SSN, loan or Debt ID, and loan programs (Direct Loans, Perkins, FFEL, FISL and any loans assign to DCS). These detail records must support the monthly reports submitted to FSA Accounting.

CDDTS is classified as a Major Application. It consists of a single production server running the CDDTS application components and an Oracle database on the Windows 2000 Advanced Server operating system. The production server and associated development servers are housed in the ACS data center in Rockville, MD. The primary users of CDDTS are customer service representatives in the CDDTS Call Center in Utica, NY.

The primary users of CDDTS are the Customer Service Representatives in the CDDTS Call Center, located in Utica, NY. Additional users include the ACS project manager and support personnel. ACS system administrators have operating system access to perform maintenance functions on the server operating system, and ACS database administrators have access to the CDDTS database.

The major components of CDDTS are described below.

Software:
- CDDTS application, consisting of:
  - VisualBasic with COM objects
  - HTML pages
  - Active Server Pages

Oracle 8i database system
Windows operating system

Hardware:
Production server housed in ACS data center
Development server housed in ACS data center
Firewalls and other network components located in ACS data center
Call Center workstations located in Utica, NY

Physical facilities:
ACS data center in Rockville, MD
ACS support offices in Rockville, MD
Call Center in Utica, NY

CDDTS was deployed in three phases, with the following functionality planned for each release:

Phase 1 (July 2002)

Accept electronic transfer of loan assignment data from Direct Loans, Guaranty Agencies/FFEL, FISL (using FFEL format) and DCS.
Data entry screens capture loan assignment data from Perkins and other paper transfers.
Functionality to edit loan assignment data files
Files with errors that cannot be corrected will be returned to the sender
Records that pass the edits will be recorded in the CDDTS database
Provide Customer Service Representatives with read only view
Provide data imaging capability
Perform system backups
Provide a list of personnel that require security clearance/system access
File received documents in a storage and retrieval system.
Ability to match loans for the same borrower submitted by different lenders/guarantors using the borrower SSN
Ability to match promissory notes and Disability Discharge application documents with the correct borrower and/or loan, using the borrower SSN, note date, and original loan amount.
Ability to accept and track disability discharge applications and loan information for each borrower in a joint consolidation loan

Phase II (August 2002)

Allow CSR's to update demographic information in the database.
Ability to separately process and record voluntary and involuntary borrower payments.
Generate Initial Determination and Reinstatement letters
Generate income request notices on each anniversary date and 30 day, 60 day and 90 day follow-ups if necessary.
Interface to query NSLDS for additional borrower loans

Phase III (October 2002)

Discharge borrowers that have satisfied the conditional disability requirements.
Record discharged borrowers in an archive database.
Reinstate loans
Provide a report of borrowers that have provided income information.
Report payments to FMS.
Loan status update reporting to NSLDS.
Automated quarterly requests to NSLDS to verify that borrowers have not received a new Federal student loan.
Automated Credit Bureau reporting.
Other Reporting.

3.2 SYSTEM INTERFACES

The CDDTS is functionally connected to other FSA Major Applications, including Direct Loan, Debt Collection, and FFEL loans, through paper documents, magnetic tape, and electronic file transfers. Direct connections with CDDTS are only available through intranet ATM connections to CDDTS users in the Utica, NY Call Center, local logins to the CDDTS servers, and remote network connections used for system and application administration.

CDDTS is a closed system and is not directly connected to EDNet or to the Internet. Remote administration of CDDTS is performed from the Rockville ACS environment using PCAnywhere and Microsoft Terminal Services. About six people are permitted to log in remotely (i.e., from home or other external locations.) All remote administration connections are through a Shiva VPN site, which requires a separate login via a dial-up line or and Internet connection.

Department of Education systems are on separate subnets defined by firewalls and routers within the ACS environment. Access control lists on the firewalls and routers limit traffic to authorized sources and destinations. All FSA development systems are also isolated from other ACS environments.

Authentication to CDDTS is by way of a user ID and password. System administrators require a separate user ID and password for access to the CDDTS operating system that is separate from authentication to the CDDTS system itself.

Figure 2 shows the CDDTS production network.

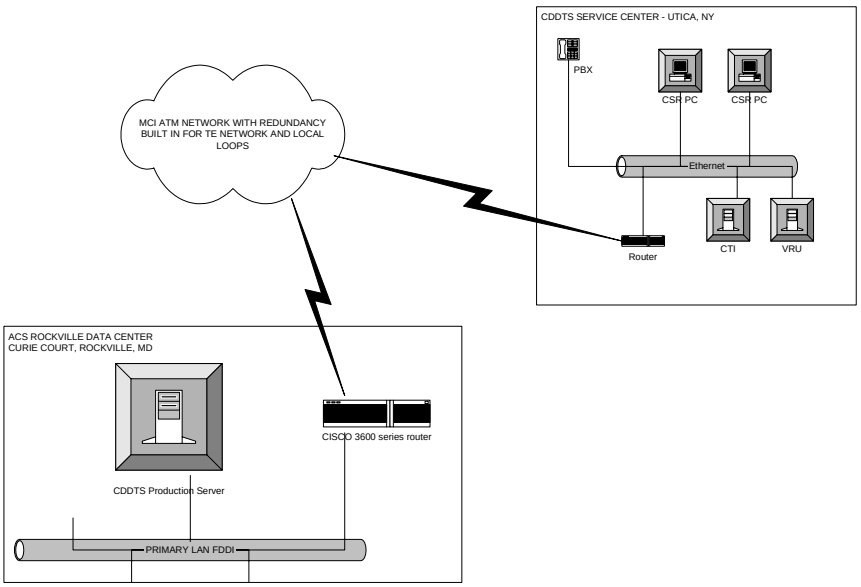

Figure 2: CDDTS Production Network

Figure 3 shows the ACS Rockville Data Center network topology, including the major network devices that provide network segmentation and firewall controls.

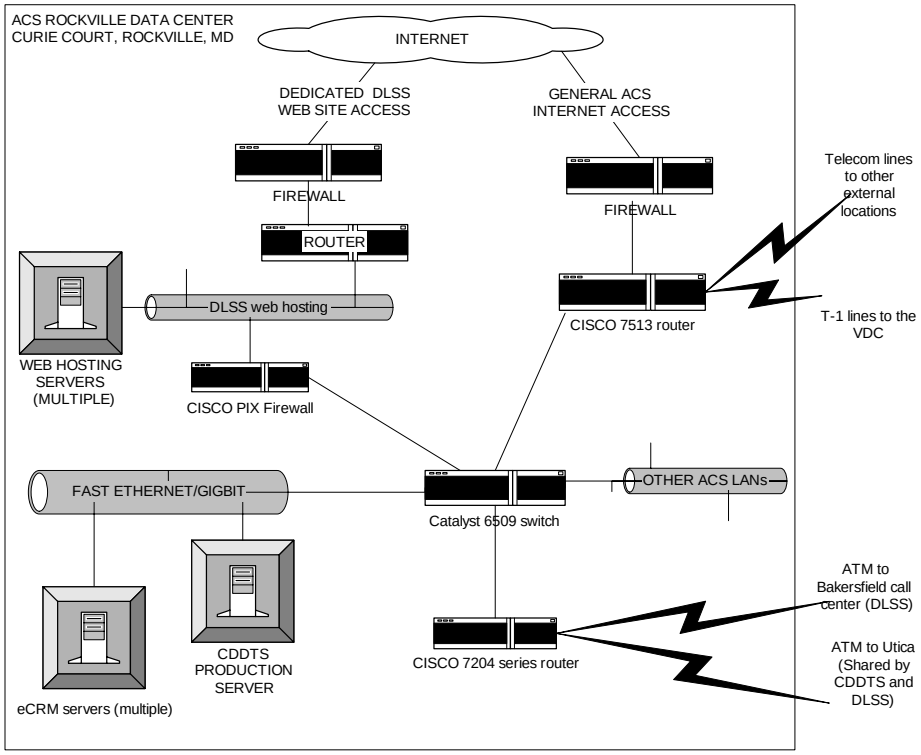

Figure 3. ACS Rockville Data Center network.

3.3 DATA

CDDTS stores and processes information about borrowers, loans, and the disabilities that are the basis for discharge of loans. Privacy act data stored and processed by CDDTS includes personal information (e.g., name and SSN) and financial information (income, loan details). CDDTS may also contain sensitive medical information used to determine the nature of severity of a borrower's disability.

3.4 SYSTEM AND DATA CRITICALITY AND SENSITIVITY

3.4.1 Criticality

CDDTS is classified as a Mission Important system. Failure of CDDTS would not preclude FSA from accomplishing core business functions in the short term (e.g., over the course of a few hours.) A failure of CDDTS that lasts from a few days to a few weeks would seriously affect FSA operations. The system serves as a backup source for mission critical data. CDDTS produces information and results that affect several other FSA applications and user groups, such as various loan holder communities, Guarantee Agencies, schools, and Department of Education regional offices.

3.4.2 Sensitivity

The criteria used to measure a system's sensitivity include confidentiality, integrity, and availability. The sensitivity areas for CDDTS are described below.

3.4.2.1 Confidentiality: **High**

The sensitivity of CDDTS data in the area of Confidentiality is High. CDDTS contains student loan information and Privacy Act data. Disclosure of CDDTS data to unauthorized individuals or institutions could possibly cause financial loss for the individual and result in legal action for liability claims. Disclosure of CDDTS data would not likely result in major financial loss, personal injury, or loss of life.

3.4.2.2 Integrity: **Medium**

The sensitivity of CDDTS data in the area of Integrity is Medium. CDDTS data integrity must be maintained to provide accuracy and completeness for tracking disability information, financial status of the individual, and loan discharge status. Destruction or unauthorized modification of CDDTS information would require effort on the part of FSA staff to recover or correct the affected information. The result would be inconvenience to FSA staff and borrowers, but all vital CDDTS information is backed up by paper documentation or electronic information stored on magnetic storage devices or optical devices.

3.4.2.3 Availability: **Medium**

The sensitivity of CDDTS information in the area of Availability is Medium. The availability of CDDTS information is of moderate concern. CDDTS information is not required to be continuously available by users, staff, or borrowers. CDDTS information must be available within a minimum of four or five days. In the event the CDDTS application or data becomes unavailable, recovery of CDDTS data from off-site backup tapes will be sufficient to carry on with limited operational needs.

The table below summarizes the sensitivity levels. The overall system sensitivity level is determined by the highest value in the CDDTS Level column. Therefore, the overall sensitivity level for CDDTS is **High.**

Sensitivity Class	CDDTS Level
Confidentiality	High
Integrity	Medium
Availability	Medium

Table 7: Sensitivity Rating

3.5 USERS

Access to the CDDTS system is restricted to users with access to the appropriate ACS Intranet server. The CDDTS application cannot be accessed over the public Internet. Additionally, the user's local Host file must contain the appropriate IP address in order to access the login screen.

No Department of Education staff routinely access CDDTS.

The major categories of CDDTS users are:

- Security Administrator: Defines application process and roles for the application
- Supervisor: Establishes and manages Production environment User IDs and passwords
- User (CSR): Accesses the CDDTS system through an assigned User ID and Password

Other users to components of CDDTS include:

- System administrators: Perform server and operating system maintenance functions.
- Network administrators: Perform network maintenance activities for ACS network segments containing the CDDTS servers.
- Database administrators: Perform database maintenance functions for the Oracle database that is a component of CDDTS.

4.0 THREAT STATEMENT

4.1 THREAT SOURCES

A threat is any instance that could disrupt the ability of CDDTS to fulfill its purpose. The four major categories of threats stem from nature, inadequate environmental controls, acts by individuals, and administrative. Examples are categorized and listed in the table below.

Natural Disaster			
Storm damage (e.g., flood, rain, snow, tornado)	Fire	Lightning strikes	Earthquakes

Environmental Control Failures				
Long-term power failure	HVAC Failures	Pollution	Liquid leakage	Biological/chemical terrorism

Human Acts		
Assault on an employee	Arson	Blackmail
Bomb/terrorism	Browsing of privacy and proprietary information	Civil disorder
Corrupted data input	Distributed Denial of Service	Economic exploitation
Falsified data input	Fraud	Hacking
Impersonation	Interception	Labor dispute/strike
Malicious code	Negligence/human error	Packet-sniffing
Password-guessing (e.g., dictionary attack, brute force attack)	Web defacement	Sabotage/vandalism
Spoofing	System tampering	Theft
Unauthorized disclosure and modification of sensitive information	Virus implant	
Administrative threats		
Inspector General	GAO	OMB
Department	Congress	NIST

Table 8: Threat Sources

4.2 THREAT ACTIONS

FSA believes human threat agents or individuals—authorized and unauthorized—to be the biggest potential threats to its systems and its data. Humans could cause intentional or unintentional damage to almost any FSA system, potentially impairing the ability of it systems to operate effectively. Possible human threat agents include:

- Insiders, disgruntled employees, dishonest employees, malicious persons,
- Authorized users (e.g., privileged system users, such as DBA, system administrator, computer operator; and unprivileged system users and application users),
- Terminated employees, including retired, resigned, or fired employees,
- Contractors and subcontractors (e.g., cleaning crew, technical support personnel, developers, and computer and telephone service repair staff),
- Foreign chair companies or foreign governments with an interest in the information held in the system, and
- Unauthorized users, who may use hacking or penetration techniques against an FSA system or EDNet with the malicious intent of disrupting normal operations and causing harm to a system (e.g., computer criminals, terrorists, hackers, intruders, Internet users, perpetrators).

5.0 FINDINGS

CDDTS processes and stores sensitive personal, medical, and financial information. However, since CDDTS consists few systems components, and is accessed by a relatively small number of users, many of the risks it faces are lower than would be the case for more complex FSA systems with more users. This section documents the findings and observations made during the CDDTS security assessment. In many cases, the findings should be corrected by actions that are already planned or scheduled (e.g., M3 – M6). Other findings represent situations that need to be tracked but represent no immediate impact or can be easily corrected (M8, A2, A3). All of the findings rated as High Risk are technical issues that will require design review.

The number and severity of risk for each category of observation was:

Category	High	Medium	Low
Management	-	7	2
Operational	-	1	-
Technical	4	4	-
Administrative	-	3	-
Totals	**4**	**15**	**2**

Appendix A of this document represents the detailed findings of the risk assessment performed on CDDTS. An observation resulted when vulnerability was identified with a threat that could exploit the vulnerability. Several methods were employed to identify vulnerabilities to the system from documentation reviews to vulnerability scans. Each of the observations is listed and numbered singularly in the appendix. The presentation of each observation consists of the following:

- Prioritized number of the observation,
- Detailed description of the vulnerability,
- A list of the threat(s) identified in the "N-E-H-A" category,
- An impact assessment of the likelihood that a vulnerability will be exploited by a threat and the impact on CDDTS of successful exploitation,
- An assessment of the level of risk to CDDTS based on the threat and vulnerability assessment, and
- A recommendation of countermeasures that would reduce or eliminate the risk.

The table below summarizes the assessment findings and their risk level. Appendix A contains the Risk Assessment Findings Matrix that presents detailed information about the vulnerability findings, threat descriptions, risk calculations, and proposed countermeasures. Appendix B shows the FSA Baseline Security Requirements with annotation of initial findings identified during the assessment.

OBSERVATION NUMBER	VULNERABILITY DESCRIPTION	RISK LEVEL
Management Security		
M1	Security testing of changes is not part of the CDDTS configuration management plan.	Medium
M2	Anti-virus tools are not run on the CDDTS server.	Medium
M3	Security training during employee orientation is brief and not documented.	Medium
M4	Disaster recovery plans have not been tested.	Medium
M5	Business continuity plans have not been tested.	Medium
M6	A security training and awareness program has not been fully implemented.	Medium
M7	Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a third party.	Medium
M8	Security risk analysis and testing is not included in the configuration management plan.	Low
M9	Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.	Low
Operational Security		
O1	Authorized access is not reviewed annually.	Medium
Technical Security		
T1	Audit trail logging and review are not routinely performed.	High
T2	User passwords for the CDDTS application are stored in clear text.	High
T3	There are no functions to detect and lock accounts after repeated login failure.	High
T4	The System Security Plan does not specify periodic scanning for unauthorized modems.	High
T5	An Intrusion Detection System is not yet fully implemented.	Medium
T6	Firewall policies and filtering rules should be audited.	Medium
T7	CDDTS accounts are not configured for automatic logout after periods of inactivity.	Medium
T8	Some file transfers to CDDTS are made through standard FTP.	Medium
Administrative Security		
A1	No CDDTS asset inventory.	Medium
A2	A FISMA Privacy Impact Assessment not performed.	Medium
A3	The System Security Plan is missing required content.	Medium